

Amendments to the Specification:

Please amend the paragraph beginning on line 4 of page 6 of the application to read as follows:

A preferred path may be, for example, a path associated with a tunnel or with an IP sub-net assigned to a specific path.

Please amend the paragraph beginning on line 28 of page 6 of the application to read as follows:

Fig. 2(a) is a flow chart of a method performed by the embodiment of Fig. 1(a). In element 202, end system 104 initiates an IP flow to another end system outside of edge IP network 102. In this example, there is no routing information in routing table 107 for the packet and the packet is thus routed over default connection 110, which is monitored by IP flow monitor 108. In element 204, IP flow monitor 108 copies the destination information from the first packet in the IP flow and sends the destination information 126 from that packet to IP route comparator 130. The IP packet is transmitted on the default path because the IP route injector has not updated the route table (RT) 107 in the router (Router 1) 106.

Please amend the paragraph beginning on line 12 of page 7 of the application to read as follows:

If the destination information 126 is found in the prefix table of IP route comparator 130 then, in element 208, IP route comparator 130 sends the matching preferred destination information 136 to IP route injector 140. In element 210, IP route injector 140 sends updated routing information based on the entry from the route comparator 130 to all routing tables used by routers connecting the edge IP network to other IP networks. Lastly, in element 212, router 106 redirects all subsequent packets in the IP flow (in this embodiment, other packets having the same destination packet) to the path specified by IP route injector 140. Thus, subsequent packets or IP flows with the same destination information as the packet causing the update will not be processed by IP flow monitor 108 since the IP flow will no longer use the default path. In the described embodiment, the first packet of an IP flow will be routed via the default path(s) 110 (so that it can be detected by IP flow monitor

108). Subsequent packets will be routed via the preferred path(s) 120. In some embodiments, if the IP destination information does not match an entry in IP route comparator 130, a negative acknowledgement is sent to IP flow monitor 108 so that subsequent items in the current IP flow will not be forwarded to the route comparator 130. This embodiment reduces the work required of IP route comparator 180 130 since it no longer needs to check whether it should send destination information to IP route injector 190 140.

Please amend the paragraph beginning on line 28 of page 7 of the application to read as follows:

The setup of routes in the prefix table preferably is accomplished using a BGP session as known to persons of ordinary skill in the art. Each router 107 106 is configured with a BGP peer session to IP route comparator 182 130. This peer session is used to send the local subnets to the comparators, which then installs or forwards the routes to the prefix table/database. Route comparator 182 130 includes functionality to update routes in the prefix table.

Please amend the paragraph beginning on line 3 of page 8 of the application to read as follows:

Fig. 3 illustrates the sequence of events when a destination prefix is withdrawn from the prefix table. The withdrawal of routes is triggered by either withdrawal of prefixes using the BGP session from the route comparator or loss of this BGP session. The purpose of this logic is to remove the destination prefix from any caches and routing tables. The A database (such as 548 of Fig. 5) tracks which route injectors have used each prefix. When a prefix is withdrawn, every route injector that uses the prefix is notified to remove the route from the their corresponding routing table of router 1.

Please amend the paragraph beginning on line 18 of page 8 of the application to read as follows:

Fig. 2(b) 1(b) also shows how information is placed in cache 184. In the described embodiment, IP route comparator 180 always sends the destination information ~~126~~ 176 back to cache 184, whether it is in the prefix table 199 of IP route comparator 180 or not (see elements 257 and 264 of Fig. 2(b)). In the described embodiment, no acknowledgment is sent back to IP flow monitor 108 158, since the cache 184 performs the function of filtering out destination information that has already been considered by IP route comparator 180. The communication path 182 is used to remove entries from the destination cache 184 to maintain consistency between the cache 184 and the prefix table 199. Cache entries are removed from the destination cache when a prefix is added to the prefix table.

Please amend the paragraph beginning on line 8 of page 9 of the application to read as follows:

Fig. 5 is a block diagram showing a network in accordance with a fifth preferred embodiment of the present invention. (In this embodiment, IP route injector 540 is shown as being remote, although in certain embodiments, it may also be local to network 502.) In Fig. 5, each IP route comparator 530 in a network queries one or more remote databases 548 to access a prefix table(s) 550. The fact that more than one IP route comparator is capable of accessing database 548 is indicated by connection 549 in the figure. Whenever each IP route comparator 530 needs to compare received destination information ~~126~~ 526, it queries database 548 to see if a match exists. Alternately, one or more IP route comparators 530 may cache the results of their database queries locally in order to reduce the number of database accesses.

Please amend the paragraph beginning on line 17 of page 9 of the application to read as follows:

Fig. 6 shows an example of an IP packet. In the example, the IP format is written as a sequence of 32-bit “chunks.” Fields include a source IP address 602 and a destination IP

address 604. As discussed above, all packets in a particular IP flow will have the same destination address in field 604. IP flow monitor 108, in certain embodiments, also monitors information in addition to the destination address to determine when a packet belongs to a particular IP flow. This information can include, without limitation, type of service 606. For example, a current version of BGP (BGP4) includes the following types of service:

Bits 0-2: Precedence.

Bit 3: 0 = Normal Delay, 1 = Low Delay.

Bits 4: 0 = Normal Throughput, 1 = High Throughput.

Bits 5: 0 = Normal Reliability, 1 = High Reliability.

Bit 6-7: Reserved for Future Use.

Any of these type of service fields can be monitored by IP flow monitor 108 and included in the format of prefix table 149 of Fig. 1(a) or any similar prefix table.

Please amend the paragraph beginning on line 5 of page 10 of the application to read as follows:

Other information that might be monitored and included in the prefix table format include protocol type, source and/or destination port number, source IP address, diffserv bits (*i.e.*, bits associated with the Differentiated Services (diffserv) protocol. The diffserv protocol provides a framework that enables deployment of scalable service discrimination over the Internet), etc. In general, any appropriate type of information discernible from a monitored packet and useful to determining a preferred path for the packet in the subject network may be used.